



**DEPARTMENT OF THE AIR FORCE  
31ST FIGHTER WING (USAFE)**

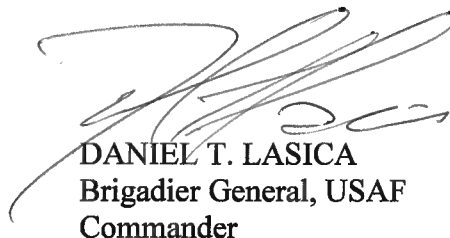
23 March 2020

**MEMORANDUM FOR ALL 31 FW PERSONNEL AND TENANT UNITS**

**FROM: 31FW/CC**

**SUBJECT: Critical Information and Indicators List (CIIL) for 31 FW Personnel and Tenant Units**

1. Critical information is specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Armed with our critical information, an opponent can take measures to cause our mission to fail, cause loss of lives, or damage friendly resources.
2. Maintaining OPSEC is a crucial element to successful mission execution. All personnel directly or indirectly involved in planning, conducting, and supporting operations, exercises, and other sensitive activities have an inherent responsibility toward the security of those operations and activities. OPSEC applies to every mission, during training and real-world operations. Adversaries may collect against any and all operations and exercises. Just as every Air Force unit contributes to the overall mission, every unit's action provides clues or indicators to the big operational picture.
3. All personnel will be familiar with the information outlined in this CIIL, as well as critical information for their respective organizations. Protecting this information is the responsibility of all 31st Fighter Wing members, as well as all tenant units and personnel assigned to Aviano AB.
4. For any questions regarding OPSEC, contact your unit level OPSEC coordinator. The POCs for the 31st Fighter Wing OPSEC Program are MSgt Jordan Scott and MSgt Michael Winnett, 31st Fighter Wing Plans and Programs. They can be reached at DSN 632-7316.



**DANIEL T. LASICA**  
Brigadier General, USAF  
Commander

**Attachment:  
31st Fighter Wing CIIL 2020**

**“Return With Honor”**



## 31st Fighter Wing Critical Information and Indicators List (CIIL) 2020

The following is a list of Critical Information, whether REAL-WORLD or EXERCISE, which must be protected from disclosure to our adversaries:

- a. Privacy Act Information, Personally Identifiable Information, and For Official Use Only
- b. DV visit information (names, ranks, itinerary, support staff composition, or security)
- c. Readiness status (strengths, capabilities, limitations, shortfalls and get-well dates)
- d. Composition & disposition of forces (strength, number, equipment, deployed location)
- e. Detailed information of personnel or equipment schedules, duty status, or itineraries
- f. Equipment and personnel movements (size, location, departure or arrival times)
- g. Budget information
- h. Operation or Exercise specific information
- i. Mission Tactics, Techniques and Procedures (TTPs)
- j. Details on critical infrastructure, nodes, links, or facilities
- k. Random Antiterrorism Measures (RAMs) details (checklist numbers, actions, times)-including EXERCISE RAMs
- l. Plans and checklists

The following measures will be employed to protect OPSEC Critical Information and indicators:

- a. 100% shredding of all documents and notes (shredders must be rated at a minimum security level P-3)
- b. Encrypt e-mails containing critical information or use secured methods for communication (i.e. classified network)
- c. Delete unnecessary email history and/or traffic before forwarding, and confirm "need to know" of all recipients
- d. Do not discuss operations outside work with family, on cell phones or social media sites
- e. Secure buildings or official areas
- f. Limit workplace discussions to "need to know" basis
- g. Use of privacy act cover sheets
- h. When printing documents, validate that there is no compilation of information which may change the classification
- i. Develop and employ methods to reduce patterns and signatures to daily activities (alternate routes, vary execution times and locations)
- j. Apply a "common-sense" test: if you think it should be protected, protect it!

**This list is not all-inclusive. It is the responsibility of all Team Aviano members to protect the critical information they use in their day-to-day mission. Everyone must be aware that what they say or type could compromise the mission.**

**UNCLASSIFIED**